Claims:

1. A system comprising:

a biometric data input device; and

a biometric verifier connected to the biometric data input device,

wherein the biometric data input device comprises:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data; and

an encoder for encoding the digital biometric data using secret information to transmit encoded data to the biometric verifier, and

the biometric verifier comprises:

a decoder for decoding the encoded data using the secret information to reproduce digital biometric data;

a verifier for verifying identity of the individual based on the digital biometric data.

2. The system according to claim 1, wherein the secret information is a unique key identifying the biometric data input device.

3. The system according to claim 2, wherein the verifier comprises:

a feature extractor for extracting a feature of the digital biometric data decoded by the decoder;

a first determiner for determining whether the feature of the digital biometric data is a registered biometric feature of an authorized user, by comparing the feature of the digital biometric data against previously registered biometric features;

a second determiner for determining whether the biometric data input device is an authorized device, based on the secret information; and

a third determiner for determining that the individual is an authorized user when the feature of the digital biometric data is a registered biometric feature of an authorized user and the biometric data input device is an authorized device.

4. A system comprising:

at least one biometric data input device; and

a biometric verifier connected to the at least one biometric data input device,

wherein each of the at least one biometric data input device comprises:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data; and

an encryptor for encrypting the digital biometric data

using an encryption key to transmit encrypted data to the biometric verifier, wherein the encryption key identifies the biometric data input device, and

the biometric verifier comprises:

a table storing an encryption key corresponding to each of said at least one biometric data input device;

a decryptor for decrypting the encrypted data using the encryption key corresponding to the biometric data input device to reproduce digital biometric data;

a comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a comparison result; and

a determiner for determining whether the individual is an authorized person, based on the comparison result and correctness of the digital biometric data decrypted by the decryptor.

5. The system according to claim 4, wherein the determiner determines the correctness of the digital biometric data decrypted by the decryptor depending on whether a type of the digital biometric data decrypted by the decryptor matches that of the digital biometric data outputted by the biometric data input device.

6. The system according to claim 4, wherein a fingerprint is used as the physical characteristic.

7. A system comprising:

at least one biometric data input device; and

a biometric verifier connected to the at least one biometric data input device,

wherein each of the at least one biometric data input device comprises:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

a watermark encoder for embedding secret information as a watermark in the digital biometric data to produce watermarked biometric data;

an encryptor for encrypting the watermarked biometric data to produce encrypted data; and

a transmitter for transmitting the encrypted data and a device identification identifying the biometric data input device to the biometric verifier, and

the biometric verifier comprises:

a table storing secret information corresponding to a device identification for each of said at least one biometric data input device;

a decryptor for decrypting the encrypted data to produce watermarked digital biometric data;

a watermark decoder for separating digital biometric data and watermark data from the watermarked digital biometric data

decrypted by the decryptor;

a first comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result;

a second comparator for comparing the watermark data separated by the watermark decoder with secret information corresponding to the device identification identifying the biometric data input device to produce a secret information comparison result; and

a determiner for determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result.

8. The system according to claim 7, wherein a fingerprint is used as the physical characteristic.

9. A system comprising:

at least one biometric data input device; and

a biometric verifier connected to the at least one biometric data input device,

wherein each of the at least one biometric data input device comprises:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

a watermark encoder for embedding secret information as

a watermark in the digital biometric data to produce watermarked biometric data;

a first encryptor for encrypting the watermarked biometric data to produce encrypted biometric data;

a second encryptor for encrypting the secret information using a public key of asymmetric encryption scheme to produce encrypted secret information; and

a transmitter for transmitting the encrypted biometric data and the encrypted secret information, and

the biometric verifier comprises:

a first decryptor for decrypting the encrypted biometric data to produce watermarked digital biometric data;

a second decryptor for decrypting the encrypted secret information to produce received secret information;

a watermark decoder for separating digital biometric data and watermark data from the watermarked digital biometric data decrypted by the decryptor;

a first comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result;

a second comparator for comparing the watermark data separated by the watermark decoder with the received secret information to produce a secret information comparison result; and

a determiner for determining whether the individual is an authorized person, based on the feature comparison result

and the secret information comparison result.

10. The system according to claim 9, wherein a fingerprint is used as the physical characteristic.

11. The system according to claim 9, wherein the biometric verifier is connected to the at least one biometric data input device via a network.

12. The system according to claim 11, wherein the encrypted biometric data and the encrypted secret information are transmitted to the biometric verifier through different channels.

13. A biometric data input device connected to a biometric verifier, comprising:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

a memory storing an encryption key identifying the biometric data input device; and

an encryptor for encrypting the digital biometric data using the encryption key to transmit encrypted data to the biometric verifier.

14. The biometric data input device according to claim

13, wherein the biometric data sensor, the memory, and the encryptor are inseparably implemented in one piece.

15. The biometric data input device according to claim 13, wherein a fingerprint is used as the physical characteristic.

16. A biometric data input device connected to a biometric verifier, comprising:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

a memory storing secret information corresponding to the biometric data input device;

a watermark encoder for embedding the secret information as a watermark in the digital biometric data to produce watermarked biometric data;

an encryptor for encrypting the watermarked biometric data to produce encrypted data; and

a transmitter for transmitting the encrypted data and a device identification identifying the biometric data input device to the biometric verifier.

17. The biometric data input device according to claim 16, wherein the biometric data sensor, the memory, and the encryptor are inseparably implemented in one piece.

18. The biometric data input device according to claim 16, wherein a fingerprint is used as the physical characteristic.

19. A biometric data input device connected to a biometric verifier, comprising:

a biometric data sensor for inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

a watermark encoder for embedding secret information as a watermark in the digital biometric data to produce watermarked biometric data;

a first encryptor for encrypting the watermarked biometric data to produce encrypted biometric data;

a second encryptor for encrypting the secret information using a public key of asymmetric encryption scheme to produce encrypted secret information; and

a transmitter for transmitting the encrypted biometric data and the encrypted secret information.

20. The biometric data input device according to claim 19, wherein a fingerprint is used as the physical characteristic.

21. A biometric verifier connected to at least one

biometric data input device, comprising:

a table storing an encryption key corresponding to each of said at least one biometric data input device;

a decryptor for decrypting encrypted data using the encryption key corresponding to a biometric data input device to reproduce digital biometric data, wherein the encrypted data is received from the biometric data input device;

a comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a comparison result; and

a determiner for determining whether the individual is an authorized person, based on the comparison result and correctness of the digital biometric data decrypted by the decryptor.

22. A biometric verifier connected to at least one biometric data input device, comprising:

a table storing secret information corresponding to a device identification for each of said at least one biometric data input device;

a decryptor for decrypting encrypted data to produce watermarked digital biometric data, wherein the encrypted data is received from a biometric data input device;

a watermark decoder for separating digital biometric data and watermark data from the watermarked digital biometric data decrypted by the decryptor;

a first comparator for comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result;

a second comparator for comparing the watermark data separated by the watermark decoder with secret information corresponding to the device identification identifying the biometric data input device to produce a secret information comparison result; and

a determiner for determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result.

23. A biometric verifier connected to at least one biometric data input device, comprising:

a first decryptor for decrypting encrypted biometric data to produce watermarked digital biometric data, wherein the encrypted data is received from a biometric data input device;

a second decryptor for decrypting encrypted secret information to produce received secret information, wherein the encrypted secret information is received from the biometric data input device;

a watermark decoder for separating digital biometric data and watermark data from the watermarked digital biometric data decrypted by the decryptor;

a first comparator for comparing a feature of the

digital biometric data against previously registered biometric features to produce a feature comparison result;

a second comparator for comparing the watermark data separated by the watermark decoder with the received secret information to produce a secret information comparison result; and

a determiner for determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result.

24. In a system comprising: a biometric data input device; and a biometric verifier connected to the biometric data input device, a method for verifying identity of an individual, comprising the steps of:

at the biometric data input device,

a) inputting as biometric data a physical characteristic of an individual to produce digital biometric data; and

b) encoding the digital biometric data using secret information to transmit encoded data to the biometric verifier, and

at the biometric verifier,

c) decoding the encoded data using the secret information to reproduce digital biometric data;

d) verifying identity of the individual based on the digital biometric data.

25. The method according to claim 24, wherein the step (d) comprises the steps of:

extracting a feature of the digital biometric data decoded by the decoder;

determining whether the feature of the digital biometric data is a registered biometric feature of an authorized user, by comparing the feature of the digital biometric data against previously registered biometric features;

determining whether the biometric data input device is an authorized device, based on the secret information; and

determining that the individual is an authorized user when the feature of the digital biometric data is a registered biometric feature of an authorized user and the biometric data input device is an authorized device.

26. In a system comprising: a biometric data input device; and a biometric verifier connected to the biometric data input device, a method for verifying identity of an individual, comprising the steps of:

at the biometric data input device,

a) inputting as biometric data a physical characteristic of an individual to produce digital biometric data; and

b) encrypting the digital biometric data using an

encryption key to transmit encrypted data to the biometric verifier, wherein the encryption key identifies the biometric data input device, and

at the biometric verifier,

c) storing an encryption key corresponding to each of said at least one biometric data input device;

d) decrypting the encrypted data using the encryption key corresponding to the biometric data input device to reproduce digital biometric data;

e) comparing a feature of the digital biometric data against previously registered biometric features to produce a comparison result; and

f) determining whether the individual is an authorized person, based on the comparison result and correctness of decrypted digital biometric data.

27. The method according to claim 26, wherein, in the step (f), the correctness of the decrypted digital biometric data is determined depending on whether a type of the decrypted digital biometric data matches that of the digital biometric data outputted by the biometric data input device.

28. In a system comprising: a biometric data input device; and a biometric verifier connected to the biometric data input device, a method for verifying identity of an individual, comprising the steps of:

at the biometric data input device,

inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

embedding secret information as a watermark in the digital biometric data to produce watermarked biometric data;

encrypting the watermarked biometric data to produce encrypted data; and

transmitting the encrypted data and a device identification identifying the biometric data input device to the biometric verifier;

at the biometric verifier,

storing secret information corresponding to a device identification for each of said at least one biometric data input device;

decrypting the encrypted data to produce watermarked digital biometric data;

separating digital biometric data and watermark data from decrypted watermarked digital biometric data;

comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result;

comparing the separated watermark data with secret information corresponding to the device identification identifying the biometric data input device to produce a secret information comparison result; and

determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result.

29. In a system comprising: a biometric data input device; and a biometric verifier connected to the biometric data input device, a method for verifying identity of an individual, comprising the steps of:

at the biometric data input device,

inputting as biometric data a physical characteristic of an individual to produce digital biometric data;

embedding secret information as a watermark in the digital biometric data to produce watermarked biometric data;

encrypting the watermarked biometric data to produce encrypted biometric data;

encrypting the secret information using a public key of asymmetric encryption scheme to produce encrypted secret information; and

transmitting the encrypted biometric data and the encrypted secret information, and

at the biometric verifier,

decrypting the encrypted biometric data to produce watermarked digital biometric data;

decrypting the encrypted secret information to produce received secret information;

separating digital biometric data and watermark data from the decrypted watermarked digital biometric data;

comparing a feature of the digital biometric data against previously registered biometric features to produce a feature comparison result;

comparing the separated watermark data with the received secret information to produce a secret information comparison result; and

determining whether the individual is an authorized person, based on the feature comparison result and the secret information comparison result.